Abstract

Computer networks are usually vulnerable to attacks by any unauthorized person trying to misuse the resources. Hence they need to be protected against such attacks by Intrusion Detection Systems (IDS). The traditional prevention techniques such as user authentication, data encryption, avoidance of programming errors, and firewalls are only used as the first line of defense. But, if a password is weak and is compromised, user authentication cannot prevent unauthorized use. Similarly, firewalls are vulnerable to errors in configuration and sometimes have ambiguous/undefined security policies. They fail to protect against malicious mobile code, insider attacks and unsecured modems. Therefore, intrusion detection is required as an additional wall for protecting systems. Previously many techniques have been used for the effective detection of intrusions. One of the major issues is however the accuracy of these systems. To improve accuracy, data mining programs are used to analyze audit data and extract features that can distinguish normal activities from intrusions. This paper shows the implementation of by viewing intrusion detection as a data mining problem. One of the most common data mining approaches i.e. classification via decision trees has been adopted to detect intrusion detection patterns.
Identifying Intrusion Patterns using a Decision Tree


http://www.wikipedia.com


Index Terms

Computer Science

Pattern Recognition
Keywords
Decision Trees  Feature Selection  Data Mining